UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/841,503	04/24/2001	Richard Alan Dayan	RPS9 2001 0011	5669

53493 7590 10/17/2005

LENOVO (SINGAPORE) PTE. LTD.
BUILDING 675, MAIL C-137
4401 SILICON DRIVE
DURHAM, NC 27709

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/841,503	**Applicant(s)** DAYAN ET AL.
	Examiner Matthew T. Henning	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 July 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 April 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

This action is in response to the communication filed on 7/1/2005.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/1/2005 has been entered.

Response to Arguments

Applicants' arguments filed 7/1/2005 have been fully considered but they are not persuasive. Applicants argues primarily that:

a. Gafken and Hasbun do not disclose comparing the similarity of the update portion with the protected partition.

b. Gafken and Hasbun did not disclose locking a protected partition in a hard drive.

c. Schneier did not teach storing the random password in a database at the server.

Regarding applicants' argument a. that Gafken and Hasbun do not disclose comparing the similarity of the update portion with the protected partition, the examiner has considered the argument and does not find the argument persuasive. Hasbun clearly teaches that the update file contains objects and the BIOS is searched for previous versions of the object (See Hasbun Col. 12 Line 59 – Col. 13 Line 17. Also see Col. 13 Line 18 – Col. 16 Line 27). This required a comparison of similarity in order to determine whether the object already existed. As such, the examiner does not find the argument persuasive.

Regarding applicants' argument b. that Gafken and Hasbun do not disclose locking a protected partition in a hard drive, the examiner has considered the argument and does not find the argument persuasive. Gafken disclosed locking the blocks of data after modification was performed (See Gafken Col. 13 Paragraph 9 – Col. 14 Paragraph 1). Furthermore, as discussed below in the rejection of claim 1 under 35 USC 103(a), it was well known in the art that a hard drive could be used in place of flash memory to store information including a BIOS. As such, it would have been obvious to replace the flash memory of Gafken and Hasbun with a partition on a hard drive. As such, the examiner does not find the argument persuasive.

Applicants' argument c. has been considered but is moot in view of the new ground(s) of rejection. See below.

All rejections and objections not specifically set forth below have been withdrawn.

Claims 1-30 have been examined, and claims 31-36 have been cancelled.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "similar" in claims 1, 11, 13, and 26 is a relative term which renders the claim indefinite. The term "similar" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. One of ordinary skill in the art would be unable to determine how alike the information in the protected partition and the portion of information stored in the update file would need to be in order to be considered "similar" to each other. As such, the ordinary person skilled in the art would be unable to determine the scope of the claim. Therefore, claims 1-30 are rejected for failing to particularly point out and distinctly claim the subject matter which the applicants regard as the invention.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

Claims 1- 4,13-19, and 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gafken (US Patent Number 6,026,016), and further in view of Hasbun et al. (U.S. Patent Number 6,088,759) hereinafter referred to as Hasbun.

Regarding claim 1, Gafken disclosed a method for updating a protected partition within a hard drive of a computing system, wherein said method comprises (See Gafken Fig. 5): starting execution of an initialization program in a processor within said computing system in response to turning on electrical power within said computing system (See Gafken Col. 3 Paragraph 2 Lines 1-4); determining whether an update partition file is stored in non-volatile storage (See Gafken Col. 5 Paragraph 5) within said computing system for subsequently updating said protected partition (See Gafken Col. 13 Paragraphs 4 and 7); after determining that said update partition is stored within said computing system for updating said protected partition, writing a portion of said update partition file to said protected partition (See Gafken Col. 13 Paragraph 8); and locking said protected partition to prevent further modification of information stored within said protected partition (See Gafken Col. 13 Paragraph 9 – Col. 14 Paragraph 1), but failed to disclose overwriting similar parts and appending new parts.

Hasbun teaches that a bios update can be allocated into virtual blocks so that the blocks can be updated individually without having to erase the entire memory first (See Hasbun Col. 5 Paragraph 6 – Col. 6 Paragraph 2 and Col. 12 Line 59 – Col. 16 Line 27). Hasbun also teaches that new blocks should be allocated from existing free memory (See Hasbun Col. 7 Paragraph 2).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Hasbun to the bios updating system of Gafken by updating each update part one at a time. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a safe method for updating a bios without risking loss of the entire bios in the event of a power failure.

Furthermore, it was well know at the time of the invention that a hard drive could be used in place of flash memory, even to store a BIOS. As such, it would have been obvious to the ordinary person skilled in the art at the time of invention to employ what was well known in the art at the time of invention in the BIOS system of Gafken and Hasbun by storing the BIOS in a hard drive instead of a flash memory. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide greater storage capacity for the BIOS and to make updating the BIOS fast and efficient.

Regarding claim 13, the combination of Gafken and Hasbun disclosed a method for updating a protected partition within a hard drive of a client computing system, wherein said method comprises: generating an update partition file within a server (See Gafken Col. 12 Paragraph 7 – Col. 13 paragraph 1, wherein it was inherent that the server created the image by signing it in order for the server to be verified through digital signatures); transferring said update partition file from said server to said client computing system (See Gafken Col. 12 Paragraph 5); storing said update partition file in non-volatile storage within said client computing system (See Gafken Col. 5 Paragraph 5); starting execution of an initialization program in a processor within said client computing system in response to turning on electrical power within said client computing system (See Gafken Col. 3 Paragraph 2 Lines 1-4); determining that said update partition file is stored in non-volatile storage within said client computing system (See Gafken Col. 13 Paragraphs 4 and 7); writing a portion of said update partition file to said protected partition (See Gafken Col. 13 Paragraph 8); and locking said protected partition to prevent further modification of information stored within said protected partition (See Gafken Col. 13 Paragraph 9 – Col. 14 Paragraph 1). The combination of Gafken and Hasbun further disclosed comparing information stored in said protected partition with information within said update partition file; when a matching portion of said information stored in said protected partition is found to be similar to said entry, said matching portion is overwritten with said entry if space around said matching portion is sufficient, and when a matching portion of said information stored in said protected partition is not found to be similar to said entry, said entry is appended to said information stored in said protected partition if space within said protected partition is sufficient (See the rejection of claim 1 above).

Claim 26 recites a computer system comprising: a processor executing an initialization program in response to power being turned on in said computer program (See Gafken Fig. 1

Element 110); a hard drive having a protected partition blocked during execution of an initialization program to prevent changing information stored within said protected partition (See Fig. 1 Element 130); non-volatile storage storing an update partition data structure for modifying contents of said protected partition and said initialization program, wherein said initialization program executing within said processor determines that said update partition data structure is stored in said non-volatile storage, writes a portion of said update partition data structure to said protected partition, and locks said protected partition to prevent further modification of information stored within said protected partition (See rejection of claim 1 above). The combination of Gafken and Hasbun further disclosed comparing information stored in said protected partition with information within said update partition file; when a matching portion of said information stored in said protected partition is found to be similar to said entry, said matching portion is overwritten with said entry if space around said matching portion is sufficient, and when a matching portion of said information stored in said protected partition is not found to be similar to said entry, said entry is appended to said information stored in said protected partition if space within said protected partition is sufficient (See the rejection of claim 1 above).

Regarding claims 2, 17, and 27, the combination of Gafken and Hasbun disclosed that a flag bit is set in non-volatile storage within said computing system when said update partition file is stored at a predetermined location in non-volatile storage within said computing system (See Gafken Col. 13 Paragraphs 3-4), and determining whether said update partition is stored within said computing system for updating said protected partition is performed by determining whether said flag bit is set (See Gafken Col. 13 Paragraph 7 and Fig. 5 Step 550).

Regarding claims 3, 18, and 28, the combination of Gafken and Hasbun disclosed that after determining that said update partition file is stored within said computing system for updating said protected partition, verifying whether said update partition file has been generated by a trusted server system, and said portion of said update partition is written to said protected partition only following verification that said update partition file has been generated by a trusted server system (See Gafken Col. 12 Paragraph 6 – Col. 13 Paragraph 1 and Figure 6).

Regarding claim 4, the combination of Gafken and Hasbun disclosed that verification that said update partition file has been generated by said trusted server system includes: forming a first message digest by applying a hash algorithm to a portion of said update partition file; forming a second message digest by decrypting a digital signature within said update partition file using a public key of said trusted server system; and determining that said first and second message digests are identical (See Gafken Col. 12 Paragraph 7 Line 10 – Col. 13 Line 2).

Regarding claim 14, the combination of Gafken and Hasbun disclosed that the update partition file is transferred from said server to said client computing system by means of electrical signals transmitted through a public switched telephone network (See Gafken Col. 4 Paragraph 7 wherein it was inherent that the update file was received through the wireless transmitter, and therefore through a public switched telephone network).

Regarding claim 15, the combination of Gafken and Hasbun disclosed that update partition file is transferred from said server to said client computing system by means of electrical signals transmitted over a local area network (See Gafken Col. 12 Paragraph 5).

Regarding claim 16, the combination of Gafken and Hasbun disclosed that transferring said update partition file from said server to said client computing system includes: writing said update partition file to a removable computer readable medium from said server; transporting said removable computer readable medium from said sever to said client computing system; and reading said update partition file from said removable computer readable medium into said client computing system (See Gafken Col. 12 Paragraph 5 wherein it was inherent that the image was stored to a floppy disk and retrieved from the floppy disk in order for the image to have been obtained through a floppy drive).

Regarding claim 19, the combination of Gafken and Hasbun disclosed the use of digital signatures to verify the origin of the update file (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

Claims 5, 6, 20-21, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Gafken and Hasbun as applied to claims 3 and 18 above, and further in view of Menezes et al. ("Handbook of Applied Cryptography") hereinafter referred to as Menezes.

Regarding claims 5 and 20, the combination of Gafken and Hasbun disclosed the use of digital signatures, including public and private keys, in order to verify that a valid server generated the boot image (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1), but the combination of Gafken and Hasbun failed to disclose the use of a password in the signature. However, the combination of Gafken and Hasbun did disclose the use of password challenges.

Menezes teaches that providing a sequence number (password), stored and updated at both a receiver and a sender, in a digital signature of the sender, protects the signature against replay attacks (See Menezes Page 399 Section (ii).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Menezes to the validation signatures of the combination of Gafken and Hasbun by providing a sequence number in the signature of the update image. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide protection against illicitly signed updates.

Regarding claims 6 and 21, the combination of Gafken, Hasbun, and Menezes disclosed that the data includes said version of said setup password appended to a portion of said update partition file (See rejection of claim 5 above), said algorithm is a hash algorithm generating a message digest (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1), and verifying that said update partition file has been generated by said trusted server system includes applying said hash algorithm to said setup password stored within said computing system appended to a portion of said update partition file to generate a first version of a message digest and comparing said first version of said message digest with a second version of said message digest obtained by signing said encrypted portion of said update partition file (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

Claims 7, 8, 11, 22, 23, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Gafken and Hasbun as applied to claims 1, 13, and 28 above, and further in view of Hayashi et al. (US 2001/0039651 A1) hereinafter referred to as Hayashi.

Regarding claims 7, 22, and 29, the combination of Gafken and Hasbun disclosed digitally signing the update file and verifying the signature prior to updating the partition (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1), but the combination of Gafken and Hasbun failed to disclose encrypting portions of the file separately and verifying each portion individually.

Hayashi teaches a method for providing a variety of software safely by breaking the file into pieces and decrypting each piece separately (See Hayashi Page 1 Col. 2 Paragraphs 3-10).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Hayashi to the updating system of the combination of Gafken and Hasbun by encrypting parts of the file separately from the other parts. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide users with customized software without imposing too much of a load on the provider. In this combination, it would also be obvious that each block contained information to be stored in a different location from the other blocks. This would have been obvious because the ordinary person skilled in the art would have been motivated not perform unnecessary computation during the update.

Regarding claim 8, the combination of Gafken, Hasbun, and Hayashi disclosed forming a first message digest by applying a hash algorithm to said entry, and forming a second message digest by signing said encrypted element associated with said entry using a public key of said trusted server system, and determining that said first and second message digests are identical (See Gafken Col. 12 Paragraph 7 Line 10 – Col. 13 Line 2).

Regarding claim 11, the combination of Gafken, Hasbun, and Hayashi disclosed that information stored in said protected partition is compared to each entry in said plurality of entries within said update partition, when a matching portion of said information stored in said protected partition is found to be similar to said entry, said matching portion is overwritten with said entry if space around said matching portion is sufficient, and when a matching portion of said information stored in said protected partition is not found to be similar to said entry, said entry is appended to said information stored in said protected partition if space within said protected partition is sufficient (See the rejection of claim 1 above).

Regarding claim 23, the combination of Gafken, Hasbun, and Hayashi disclosed that each encrypted element is formed in said server by applying a hash algorithm to said entry, forming a first message digest, and by signing said first message digest with a private key of said server; and verification that said entry has been generated by said server includes forming a second message digest by applying a hash algorithm to said entry, forming a third message digest by signing said encrypted element associated with said entry using a public key of said server, and determining that said second and third message digests are identical (See Gafken Col. 12 Paragraph 7 Line 10 – Col. 13 Line 2).

Claims 9, 10, 24-25, 30-32, and 34-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Gafken, Hasbun, and Hayashi as applied to claims 7, 22 and 29 above, and further in view of Menezes.

Regarding claim 9, Gafken, Hasbun and Hayashi disclosed the use of digital signatures, including public and private keys, in order to verify that a valid server generated the boot image parts (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1), but Gafken, Hasbun, and Hayashi did not disclose the use of a password in the signature. However, Gafken, Hasbun and Hayashi did disclose the use of password challenges (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

Menezes teaches that providing a sequence number (password), stored and updated at both a receiver and a sender, in a digital signature of the sender, protects the signature against replay attacks (See Menezes Page 399 Section (ii).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Menezes to the validation signatures of the combination of Gafken and Hasbun by providing a sequence number in the signature of the update image. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide protection against illicitly signed updates.

Regarding claim 10, the combination of Gafken, Hasbun, Hayashi, and Menezes disclosed that the data includes said version of said setup password appended to a said entry (See rejection of claim 5 above), said algorithm is a hash algorithm generating a message digest, and verifying that said entry has been generated by said trusted server system includes applying said hash algorithm to said setup password stored within said computing system appended said entry to generate a first version of a message digest and comparing said first version of said message digest with a second version of said message digest obtained by signing said encrypted element (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

Regarding claim 24, the combination of Gafken, Hasbun, Hayashi, and Menezes disclosed that a setup password is stored in non-volatile storage within said client computing system; a copy of said setup password is stored in a database accessed by said Server (See rejection of claim 5 above); said encrypted element of said update partition file is prepared in said server by signing, with a private key of said server, a result of the application of an algorithm to data including said copy of said setup password', and verification within said client computing system that said entry has been generated by said server includes signing said encrypted element associated with said entry with said public key of said server (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

Claim 25 is rejected for the same reasons as claim 10 above as applied to claim 24 above.

Regarding claim 30, the combination of Gafken, Hasbun, Hayashi, and Menezes disclosed that the non-volatile storage additionally stores a setup password, and each said encrypted element includes a digital signature signed by said trusted server system, wherein said digital signature is formed by applying a hash algorithm to an entry associated with said encrypted element to form a message digest and by signing said message digest with a private key of said trusted server system (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Gafken and Hasbun as applied to claim 1 above, and further in view of Schmidt (U.S. Patent Number 5,826,015).

The combination of Gafken and Hasbun disclosed a secure bios updating system (See rejection of claim 1 above) but failed to disclose requiring a user to input a password to unlock the bios write capabilities. However, Gafken and Hasbun did disclose the use of password challenges (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

Schmidt teaches that in order to remotely upgrade a bios, an administrator password should be provided in order to unlock the partition (See Schmidt Fig. 9 and abstract).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schmidt to the bios updating system of Gafken by requiring a correct password to be entered in order to unlock the bios altering capabilities. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the current bios from accidental or illicit alterations.

Conclusion

Claims 1-30 have been rejected, and claims 31-36 have been cancelled.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

i. Arnold et al. (US Patent Number 5.128.995) disclosed a system in which a BIOS was stored in a locked portion of a Hard Drive in order to update the BIOS more easily.

ii. Harmer (US Patent Number 5,835,760) disclosed a system which stores a BIOS in a Hard Drive and searches for portions in the BIOS to update.

iii. Zinger et al. (US Patent Number 6,836,847) disclosed that a Hard Drive could be used in place of Flash Memory.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Examiner
Art Unit 2131
9/29/2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100